

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A system for Multimedia authentication of a user equipment accessing a Multimedia domain through an access network, comprising:

subscriber server for first authenticating said user equipment within said access network, said subscriber server authorizing said user equipment to gain access to said access network wherein said subscriber server storing authentication data associated with said user equipment;

means for selectively deciding that whether an implicit authentication between the user equipment and a serving call session control function (S-CSCF) of the Multimedia domain can take place based on said first authentication of the user equipment by the access network; and

in response to a decision that said implicit authentication can take place, further comprising means for instructing the S-CSCF in the Multimedia domain that implicit authentication of the user equipment can take place by re-using said authentication data stored in the subscriber server and to not perform any explicit authentication between said S-CSCF and said user equipment; otherwise

in response to a decision that no implicit authentication can take place, further comprising means for explicitly authenticating the user equipment by issuing an authentication challenge message from the S-CSCF to the user equipment.

2. (Original) The device of claim 1, wherein the means for deciding that an implicit authentication can take place includes

means for determining the potential security of the signalling path to access the Multimedia domain through said access network.

3. (Previously Presented) The device of claim 1, wherein the means for instructing the S-CSCF that the implicit authentication can take place includes means for indicating that the final decision is on the user equipment side which can force an explicit authentication.

4. (Previously Presented) The device of claim 1, wherein the means for instructing the S-CSCF that the implicit authentication can take place includes means for indicating that this is a final decision taken by the network and no explicit authentication can be carried out.

5. (Previously Presented) The device of claim 1, further including means for notifying the user equipment that the implicit authentication of the user equipment for accessing the Multimedia domain can be carried out by the network.

6. (Previously Presented) The device of claim 1, wherein the means for deciding that the implicit authentication between the user equipment and the Multimedia domain can take place includes means for receiving a proposal of implicit authentication originated from the user equipment.

7. (Previously Presented) The device of claim 3, further comprising means for receiving an indication originating from the user equipment to confirm the acceptance of the implicit authentication proposed by the network.

8. (Previously Presented) The device of claim 7, further comprising means for indicating to the S-CSCF in charge of authenticating the user in the Multimedia domain that the user has confirmed the implicit authentication.

9. (Previously Presented) The device of claim 8, further comprising means for providing additional authentication data to said S-CSCF, said additional authentication data including at least one of

authentication type;
access information; and
authentication timestamp.

10. (Currently Amended) A user equipment enabled to obtain access to a Multimedia domain through an access network, and arranged to carry out a first explicit authentication procedure with the access network and a second explicit authentication procedure with the Multimedia domain, the user equipment comprising

means for first explicitly authenticating with a subscriber server within said access network, said subscriber server authorizing said user equipment to gain access to said access network wherein said subscriber server storing authentication data associated with said user equipment;

in response to a decision that an implicit authentication can take place between the user equipment and a S-CSCF of the Multimedia domain, means for receiving a notification ~~received~~—from the Multimedia domain indicating that an implicit authentication for the user equipment can be carried out by the network based on the first explicit authentication procedure with the access network by re-using said authentication data stored in said subscriber server and notifying the user equipment not to perform the second explicit authentication procedure with the multimedia domain;
or

in response to a decision that an implicit authentication cannot take place between the user equipment and said S-CSCF, means for receiving an authentication challenge message from the Multimedia domain for performing an explicit authentication with the user equipment.

11. (Previously Presented) The user equipment of claim 10, wherein the means for processing the notification received from the Multimedia domain includes means for receiving and processing an Implicit Authentication indication that the final decision is on the user equipment which can force an explicit authentication.

12. (Previously Presented) The user equipment of claim 11, further comprising means for sending towards the Multimedia domain an Single Sign On (SSO) enabled indication to confirm the acceptance of the implicit authentication proposed by the network.

13. (Previously Presented) The user equipment of claim 12, further comprising means for providing additional authentication data towards the Multimedia domain, said additional authentication data including at least one of

- authentication type;
- access information; and
- authentication timestamp.

14. (Previously Presented) The user equipment of claim 10, wherein the means for processing the notification received from the Multimedia domain includes means for receiving and processing the indication of Implicit Authentication by the network that the implicit authentication is a final decision taken by the network and no explicit authentication can be carried out.

15. (Currently Amended) A method for authenticating a user equipment accessing a Multimedia domain through an access network, the method comprising the steps of:

- first authenticating the user equipment with a subscriber server in the access network, said subscriber server authorizing said user equipment to gain access to said access network wherein said subscriber server storing authentication data associated with said user equipment;

registering the user equipment into the Multimedia domain, further comprising the steps of:

deciding ~~that~~ whether an implicit authentication between the user and a service call session control function (S-CSCF) of the Multimedia domain can take place based on the first authentication of the user equipment in the access network; and

in response to a decision that said implicit authentication can take place, instructing the S-CSCF in the multimedia domain that implicit authentication of the user equipment can take place by re-using ~~suing~~ said authentication data stored in the subscriber server and to not perform any explicit authentication between said S-CSCF and said user equipment; otherwise,

in response to a decision that said implicit authentication cannot take place, issuing an authentication challenge message from the S-CSCF to the user equipment to perform an explicit authentication.

16. (Previously Presented) The method of claim 15, further comprising a step of notifying from the Multimedia domain to the user equipment that implicit authentication of the user equipment for accessing the Multimedia domain can be carried out.

17. (Previously Presented) The method of claim 15, wherein the step of deciding that the implicit authentication can take place includes a step of determining the potential security of the signalling path to access the Multimedia domain through said access network.

18. (Previously Presented) The method of claim 15, wherein the step of deciding that the implicit authentication can take place includes a step of proposing from the user equipment towards the Multimedia domain an implicit authentication to be carried out between said user equipment and Multimedia domain.

19. (Previously Presented) The method of claim 15, wherein the step of instructing the S-CSCF that the implicit authentication can take place includes a step of

indicating that the Implicit Authentication is a final decision taken by the network and no explicit authentication can be carried out.

20. (Previously Presented) The method of claim 15, wherein the step of instructing the S-CSCF that the implicit authentication can take place includes a step of indicating that the final decision is on the user equipment which can force an explicit authentication.

21. (Previously Presented) The method of claim 20, further comprising a step of confirming from the user equipment acceptance of the implicit authentication proposed by the network.

22. (Previously Presented) The method of claim 21, further comprising a step of indicating to the S-CSCF in charge of authenticating the user equipment in the Multimedia domain that the user equipment has confirmed the implicit authentication.

23. (Currently Amended) A service call session control function (S-CSCF) in charge of authenticating a user equipment in the Multimedia domain when the user equipment accesses thereto through an access network where said user equipment had been previously authenticated within the access network, the serving entity comprising:

means for receiving and processing instructions originating from a subscriber server within said access network, wherein said subscriber server for performing said previous authentication of said user equipment for gaining access to said access network and for storing authentication data associated with said user equipment, said instructions indicating ~~that~~ whether an implicit authentication can take place based on the previous authentication of the user equipment by the access network and by re-using said authentication data stored in the subscriber server; and

in response to said instruction to perform said implicit authentication, means for notifying the user equipment that an implicit authentication of the user equipment for accessing the Multimedia domain can be carried out by the network and to not perform

any explicit authentication between said S-CSCF and said user equipment; otherwise,
in response to said instruction that no implicit authentication can be performed,
means for issuing an authentication challenge message from the S-CSCF to the user
equipment to perform an explicit authentication.

24. (Previously Presented) The S-CSCF of claim 23, also comprising means for receiving an indication originated from the user equipment to confirm acceptance of the implicit authentication proposed by the network.

25. (Previously Presented) The S-CSCF of claim 23, further comprising means for receiving an indication originating from the device for Multimedia authentication of the user equipment indicating that the user equipment has confirmed the implicit authentication.

26. (Previously Presented) The S-CSCF of claim 25, further comprising means for checking the matching of additional authentication data respectively received from the device for Multimedia authentication of the user equipment and from the user equipment for providing an extra security support.

27. (Previously Presented) The S-CSCF of claim 26, wherein said additional authentication data include at least one of
authentication type;
access information; and
authentication timestamp.

28. (Previously Presented) The S-CSCF of claim 23, wherein the means for notifying the user equipment that the implicit authentication can be carried out by the network includes means for indicating to the user equipment that the implicit authentication is a final decision taken by the network and no explicit authentication can be carried out.

Appl. No. 10/595,110
Amtd. Dated April 14, 2010
Reply to Office action of February 18, 2010
Attorney Docket No. P18219-US1
EUS/GJ/P/10-6034

29-34. (Cancelled)

* * *